REMARKS

This paper responds to the first Office action, which was non-final.

Claims 19-27 are rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. The Examiner's rejection is not directed to the format of the claims themselves; rather, the Examiner previously indicated that the inclusion of "transmission media" in the written description (in the paragraph bridging pages 26-27) as a type of "computer readable medium" renders the claim non-statutory. While it is true that the scope of the claims is informed by the written description, this rejection still appears to be misplaced, as it does not afford due consideration to the actual wording of the claims. The preamble of each claim recites a "computer program product in a computer readable medium," and such a medium is a "manufacture" within the meaning of 35 U.S.C. §101. Accordingly, the Examiner once again is requested to reconsider and withdraw this rejection.

Claims 1-27 are rejected under 35 U.S.C. §103(a) as being unpatentable over Grantges, Jr., U.S. Patent No. 6,324,648, in view of Datar et al, U.S. Patent No. 6,351,812, further in view of Rathbun et al, U.S. Publication No. 2003/0005308.

In response to the first office action the undersigned provided arguments distinguishing Grantges, the primary reference relied upon by the Examiner. The Examiner's final rejection found these arguments to be unpersuasive, once again taking the position that the proxy server described in the Grantges system performss certain of the functions required by the claims. For example, the Examiner at the outset states that the Grantges "proxy server parses and modifies the cookie in response to the message from [the] authorization server …" With all due respect, this argument is incorrect. The cookies described in the Grantges system (see Figure 4A) in fact are created by the gateway proxy server 40 (see, e.g., column 9, line 54+) and returned to the client for re-use as needed to obtain access to various resources; that server does not "process[] the cookie [ ]in accordance with [a] retrieved set of parameters and [any] extracted domain identifier" as required by each claim. Indeed, as previously argued, Grantges does not disclose or suggest any proxy server processing of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering. Rather, all cookies are created in the proxy server and simply returned to the client in the usual manner.

The Examiner is reminded that the subject matter of this application relates generally to a privacy proxy server or privacy service. If a user of such a system or service is very mobile and uses many different client devices, there may be occasions or environments in which the user would like to receive some or all cookies at a client device while filtering out some or all cookies in a different environment or on a different occasion, even though the user may or may not continue to employ a privacy proxy or privacy service in these different environments or upon these different occasions. For example, if a user only accesses a certain web site from the user's personal laptop and never from an office desktop, then the user may want to allow cookies through the privacy proxy server to the laptop; the laptop would tend to have the latest cookies stored in its cookie cache, which might be important for certain sites that are highly customized or individualized. In this example, the user's laptop would have recent cookies if the user decided to use the laptop without accessing the Web through the privacy proxy server. With the subject matter described herein, the user is able to create different client profiles based on the user's needs, thereby giving the user a finer granularity of control over the cookie filtering functionality of a privacy proxy server or a privacy service. With the described subject matter, the user can customize the operation of the privacy proxy server or the privacy service on the basis of the device that the user is using, on the basis of the user's location, or on the basis of some other type of user-configured category. For example, the user might have client profiles based on a type of client device, such as laptop vs. desktop vs. PDA, or based on client location, such as office vs. mobile vs. home. The subject matter disclosed herein in particular allows a user to configure a privacy proxy that is located between a client device that is being operated by the user and a server that is supporting resources that are being accessed by a user. The privacy proxy filters cookies that are returned by the server in accordance with user-configurable parameters.

To advance this prosecution, the "user-configurability" subject matter of dependent claims 4, 13 and 22 is now incorporated into the independent claims. In particular, each independent claim now positively recites the steps of receiving and storing a set of parameters, wherein the parameters comprise "domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers." As positively recited, the set of parameters are configured by the user at the client. In one illustrated embodiment, the user

interfaces (FIGs. 4A-4C) can be used for this purpose. For at least the reasons set forth above, Grantges does not teach any user-configurable options at either the application gateway proxy server 40 (at which the cookies are generated) or the DMS proxy server 34 (through which the generated cookies are passed), let alone any cookie processing.

Datar describes how a participant in an online electronic commerce transaction can validate his/her own certificate by accessing an authority that checks whether the participant's certificate is valid. If the certificate is valid, the authority passes back a cookie that includes a plurality of attributes descriptive of the certificate, namely, the identity of the certificate, a timestamp, the status of the certificate (not revoked, revoked, unknown) and, if revoked, revocation date, revocation reason, and the like, together with a digital signature of the attributes. When accessing a secure application, the participant then presents both the certificate and the cookie, obviating a real-time inquiry to the authority except in the event of a stale or missing cookie. Datar does not disclose or suggest proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering. The reference also does not teach enabling a user to receive and store "a set of parameters," where the parameters comprise "domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers."

Rathbun describes a method and system for restricting client access to a web site. In this system, a first web server receives a client login and, in response, allocates a cookie to the client that contains an access credential having at least one client-based role-based attribute. A second web server hosts the secured web site having an associated security file containing at least one client role-based access privilege. In response to the client's request at the second server, the cookie is retrieved and decoded, and the access credential is compared to the access privilege. If the credential has an attribute in common with the privilege, the client is granted access to the site. Likewise, Rathbun does not disclose or suggest proxy server filtering of a cookie that is being returned from a server to a client, let alone per-domain cookie filtering. The reference also fails to teach any user-configurability of any proxy server.

As can be seen, each prior art reference simply deals with cookie generation, and then using the cookie to obtain access to some protected resource. This is not the subject matter of the claims here. Rather, the claims here assume that the client has obtained access to the server and

that the server has issued the cookie. Unlike the cited art, the claims concern whether that cookie will be returned to the client. This cookie processing concept is not disclosed or suggested by any of the art of record, as none of the references even address the question of how a cookie being returned from a server to the client should be processed, let alone filtered according to user-configurable options. In particular, the cited prior art does not describe providing a technique for enabling a user to configure at the proxy server per-domain (and, optionally, per-client profile) filtering of cookies that are returned from servers. Rather, the cited prior art deals with an unrelated issue, *viz.*, how to process a cookie being passed from a client to the server.

For the reasons set forth above, the combination of the cited art still fails to disclose at least the following steps of claim 1:

"receiving a set of parameters in a client message at the proxy server, wherein the set of parameters are configured by the user at the client;

storing the set of parameters at the proxy server, wherein the parameters comprise domain identifiers associated with indications of whether to block transmission of cookies associated with the domain identifiers;

extracting from the response message a domain identifier associated with the server;

retrieving the set of parameters; and

processing the cookie at the proxy server in accordance with the retrieved set of parameters and the extracted domain identifier."

As the prior art does not disclose "processing the cookie" in accordance with the "retrieved set of parameters and the extracted domain identifier." This user-configurable per-source domain "filtering" provides an enhanced privacy service that is neither disclosed nor suggested by the prior art. Thus, independent claims 1 (method), 10 (apparatus) and 19 (computer program product) describe patentable subject matter.

Dependent claims 2, 11 and 20 describe the cookie filtering steps more specifically and, in particular, the steps of blocking the cookie from transmission, caching the cookie at the proxy, and sending a modified response message to the client. This is the scenario such as described in steps 614, 618 and 620 of FIG. 6A, where the user has selected an option not to allow the cookie through the privacy service proxy server. These claims are separately patentable because the

cited art does not teach any filtering of cookies being returned from a server to a client, let alone the specific requirements set forth in these claims.

Dependent claims 3, 12 and 21 likewise describe the cookie filtering steps but in this case describe the operation where the cookie (of a recognized domain) is passed back to the client. This is the scenario such as described in step 614 and 616 of FIG. 6A, where the user has selected an option to allow the cookie through the privacy service, in which case the privacy service sends the response to the client without removing or detaching the cookie from the response. These claims likewise are patentable over the cited references, which do not teach any response cookie filtering.

Dependent claims 5, 14 and 23 are separately patentable as they describe the further step of determining if the set of parameters contains an indication that the user has enabled cookie processing by the proxy server. In one embodiment, this refers to determining whether a "source domain filter enable flag" (218) is set. The cited art does not perform cookie filtering, so this functionality is also absent from any combination of the references.

Dependent claims 6, 15 and 24 are separately patentable as they describe the further steps of managing the "multiple set of parameters." This is a client profile option. The references do not disclose or suggest cookie filtering on a per-domain basis, thus they cannot teach the further features recited in these claims.

Dependent claims 7-9, 16-18 and 25-27 are patentable for the reasons advanced with respect to their parent claims.

A Notice of Allowance is respectfully requested.

Respectfully submitted,

/David H. Judson/

By: _____

David H. Judson, Reg. No. 30,467